SCRYPTOS

Trügerische Sicherheit durch SSL-Zertifikate

Relevanz ihrer Herkunft und die Konsequenzen

Detlef Hastik
Henry Frenz

SSL-Zertifikate

als „State of the Art“

Die Verwendung von SSL-Zertifikaten auf Webseiten und in Websystemen ist hochmodern. Kaum ein Anbieter verzichtet auf die verschlüsselte Übertragung seiner Inhalte zum Kunden bzw. vice versa. Immerhin verspricht die https-gesicherte Verbindung Privatsphäre und den Schutz vor Mitlesenden, die Daten missbräuchlich verwenden oder gar verfälscht einspielen könnten. Die Webbrowser belohnen die Verwendung von validen und aktuellen Zertifikaten beispielsweise mit einem beruhigenden grünen Adressbalken; der Nutzer fühlt sich prompt viel sicherer als auf einer „ungeschützten“ Seite.

Wie viel Sicherheit bedeutet https wirklich und wogegen schützt es?

SSL basiert auf dem beliebten und als sicher geltenden Public/Private-Key-Verfahren.

Der Private-Key, auch Master-Key genannt, verbleibt geschützt auf dem Server, für den das Zertifikat ausgestellt werden soll. Nur „offizielle Zertifizierer“ können SSL Zertifikate für Webseiten ausstellen, die von den – fast immer US-amerikanischen - Webbrowsern wie Chrome, Firefox, Edge, Internet Explorer oder Safari als valide akzeptiert werden. Zwar kann jedes Unternehmen und sogar Privatpersonen eigene Zertifikate ausstellen, diese werden jedoch grundsätzlich als nicht vertrauenswürdig oder sogar bösartig eingestuft. Dem unbedarften Benutzer wird empfohlen, eine solche Seite keinesfalls zu besuchen (siehe Abbildung 1).

Nicht jedes SSL-Zertifikat wird als sicher eingestuft, da echte Sicherheit nur gewährleistet werden kann, wenn der Austeller des Zertifikates garantiert, dass der „Master-Key“ keinesfalls in die Hände Dritter gelangt.

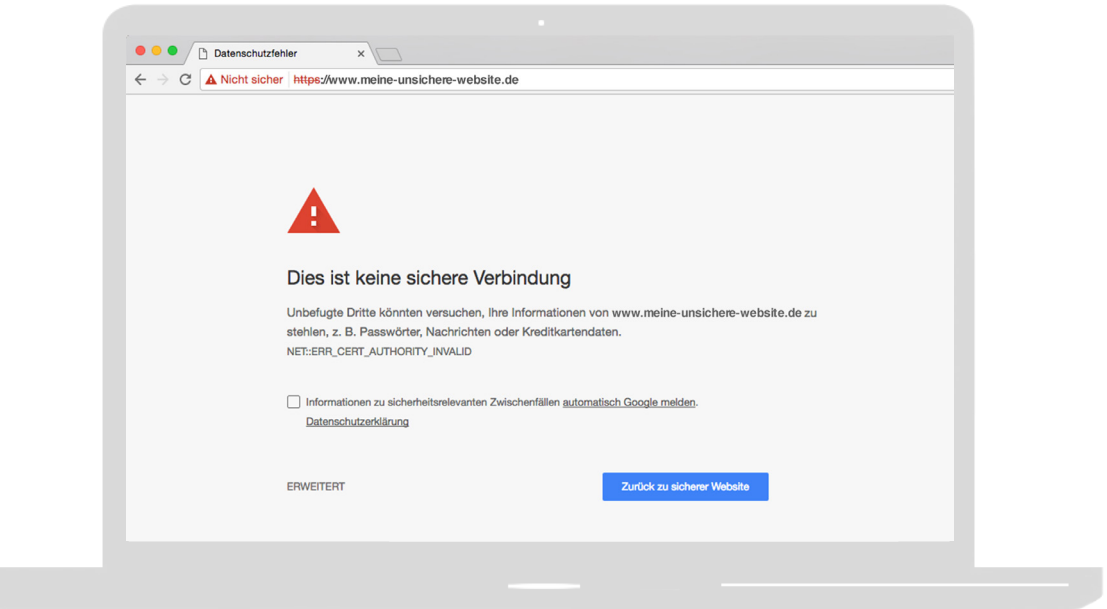

Abb. 1: Warnung vor unsicherem Zertifikat in Google Chrome

Doch wer sind eigentlich diese offiziellen Zertifizierer?

Mehr als 90% der im Internet verwendeten Zertifikate stammen von US-Unternehmen (vgl. Abbildung 2).

Der größte Anbieter, Comodo, wirbt beispielsweise mit „Creating Trust Online". Dem gegenüber steht die seit Jahren in den USA geführte Diskussion über die Legalität von Verschlüsselung und Zugriff durch die Geheimdienste.

Seit Patriot Act und FISA Amendment Act wird immer wieder versucht, von US-amerikanischen Unternehmen Hintertüren für jegliche Verschlüsselung zu erzwingen, da sie sich andernfalls der Mitschuld zu verantworten haben, falls über ihre Systeme terroristische oder anderweitig illegale Kommunikatin stattfindet.

Aktueller Stand ist der Compliance with Court Orders Act of 2016[2], der, falls er zum Gesetz wird, Hersteller elektronischer Kommunikationsgeräte, Software-Entwickler und Anbieter von Kommunikationsdiensten dazu verpflichtet, einem Gerichtsbeschluss zur Herausgabe von Informationen Folge zu leisten. Sollte es sich dabei um verschlüsselte Informationen handeln, muss die jeweilige Firma die Daten entweder entschlüsseln oder der Regierung und ihren Strafverfolgungsbehörden bei der Dechiffrierung assistieren.

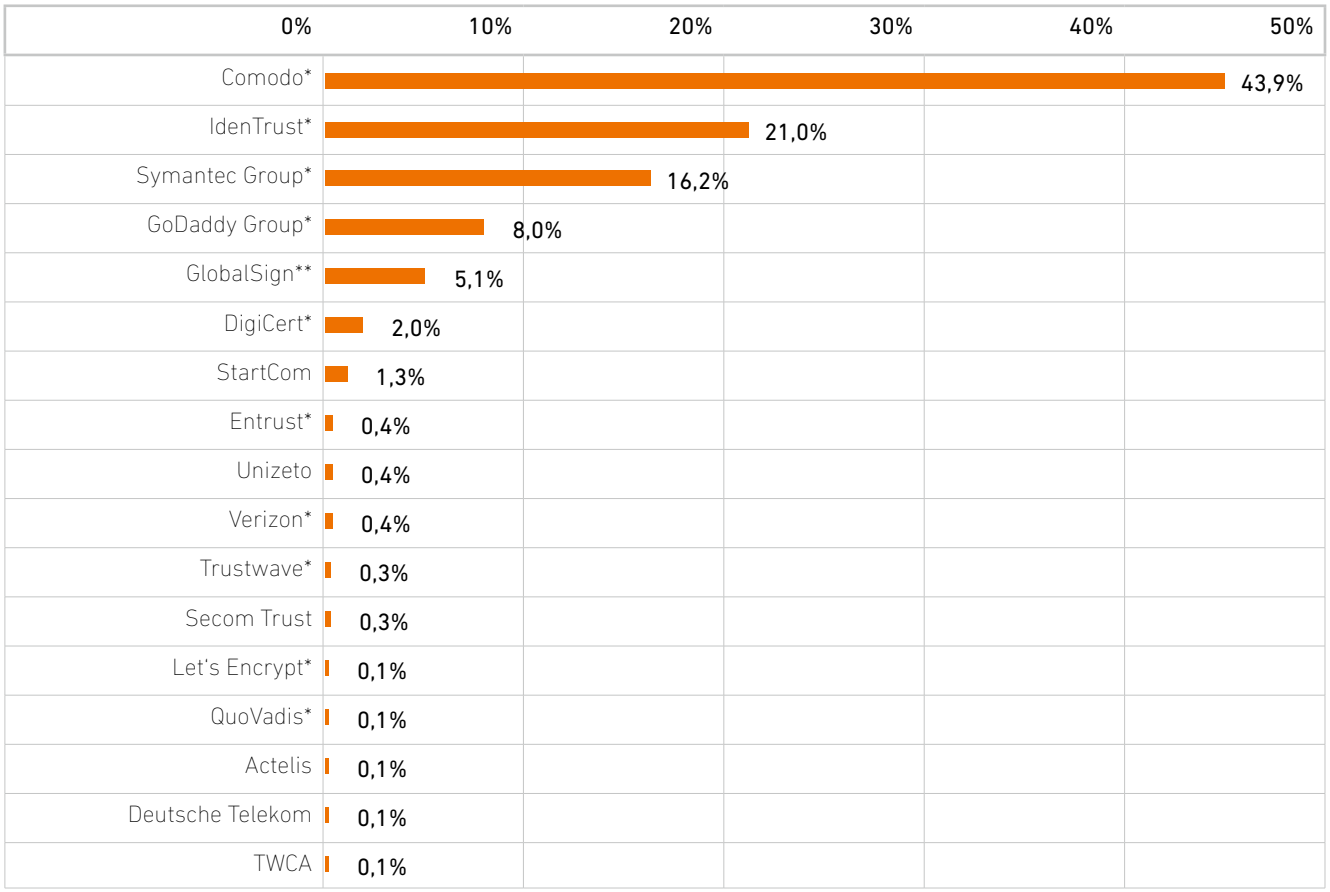

Abb. 2: Marktanteil Zertifizierer[1] (* US-Zertifizierer, ** UK-Zertifizierer)

[1] https://w3techs.com/technologies/overview/ssl_certificate/all
[2] https://de.scribd.com/doc/307378123/Burr-Encryption-Bill-Discussion-Draft

De facto müssten Firmen zukünftig, wie bereits mehrfach vom FBI gefordert, eine Hintertür einbauen oder die Verschlüsselung nur so stark auslegen, dass sie mit geringem Aufwand geknackt werden kann. Der Umkehrschluss: Verschlüsselung, die ihren eigentlichen Zweck erfüllt, Daten wirksam vor fremdem Zugriff zu schützen, wäre illegal.

In Zeiten des Protektionismus und „America first" sollte man demnach Abstand von US-amerikanischen Zertifikaten nehmen und gründlich darüber nachdenken, wo man ein Zertifikat einkauft.

Tatsächlich ist aus deutscher Sicht ein eigenes Unternehmens-Zertifikat höherwertig, als das eines wohlklingenden US-Zertifizierers wie „TeleTrust" – auch wenn der Webbrowser alles Erdenkliche tun wird, um diese Einschätzung zu torpedieren (siehe Abbildung 1).

Wenn Sie Informationen über ein SSL-Zertifikat einholen wollen, ist dies u.a. mit Firefox möglich. Klicken Sie hier auf das Icon für eine sichere Verbindung links der Adresszeile, werden Informationen zu dem verwendeten SSL-Zertifikat eingeblendet.

Darüber hinaus war es bisher überaus schwierig, vertrauenswürdige Zertifikate zu erwerben. Die Versuche für SCRYPTOS, ein D-Trust Zertifikat zu erwerben, schlugen allesamt fehl, da der Zertifizierer sich außer Stande sah, uns ein entsprechendes Zertifikat auszustellen. Es wirkte, als habe er dies noch nie getan.

Alternativ kann man Zertifikate der Deutschen Telekom AG kaufen, die jedoch Wiederverkäufer für GlobalSign ist und selbst sowohl diese, als auch VeriSign Zertifikate aus den USA einsetzt. Hier wird die Sicherheit immer wieder durch Fremdzertifikate kompromittiert.

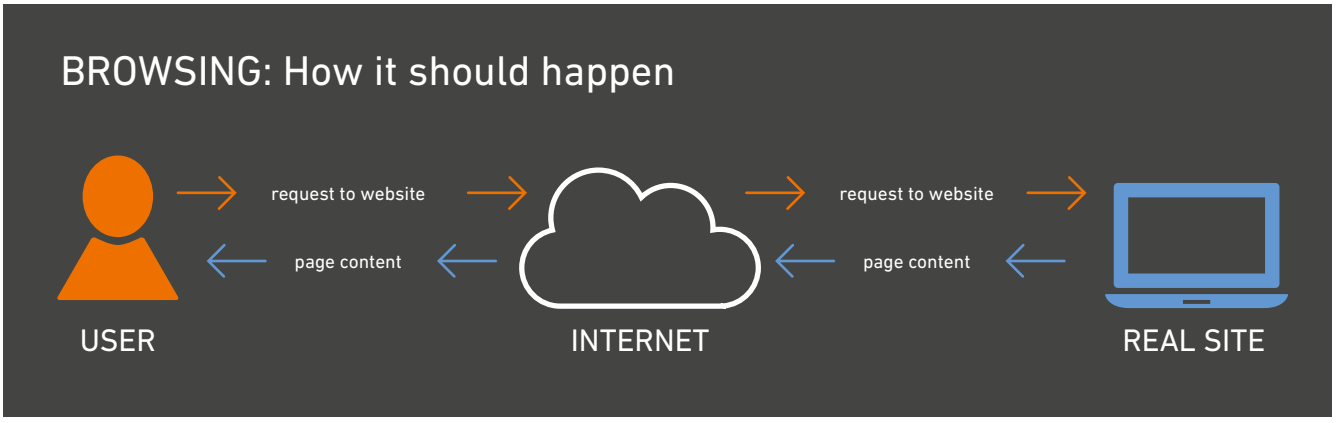

Abb. 3: Besuch einer Website im Idealfall

Was also ist zu tun?

Bisher gelten Zertifikate aus der Schweiz und aus Luxemburg als frei von Hintertüren. In der Schweiz ist die Absenz von Hintertüren bzw. Zweit-Zertifikaten für die Spionage gesetzlich geregelt, also das genaue Gegenteil der Hintertüren-Pflicht in den USA. Dies ist jedoch kein Garant auf Lebenszeit; die politische Situation, internationale Handelsabkommen und die Interessen des zertifizierenden Landes sollten immer wieder auf den Prüfstand gehoben und gegebenenfalls der Zertifizierer ausgetauscht werden.

SCRYPTOS setzt derzeit auf SwissSign Zertifikate. Die SwissSign ist eine 100%-ige Tochter der Schweizer Post. Ziel ist es sicherzustellen, dass die Verbindung zwischen Nutzer und Service immer eine 1:1 Verbindung ist (siehe Abbildung 3) und nicht durch unsichere Zertifikate unterwandert wird (sogenannte „Man in the Middle Attacke", siehe Abbildung 4), sei es durch einzelne Hacker oder die Geheimdienste anderer Staaten.

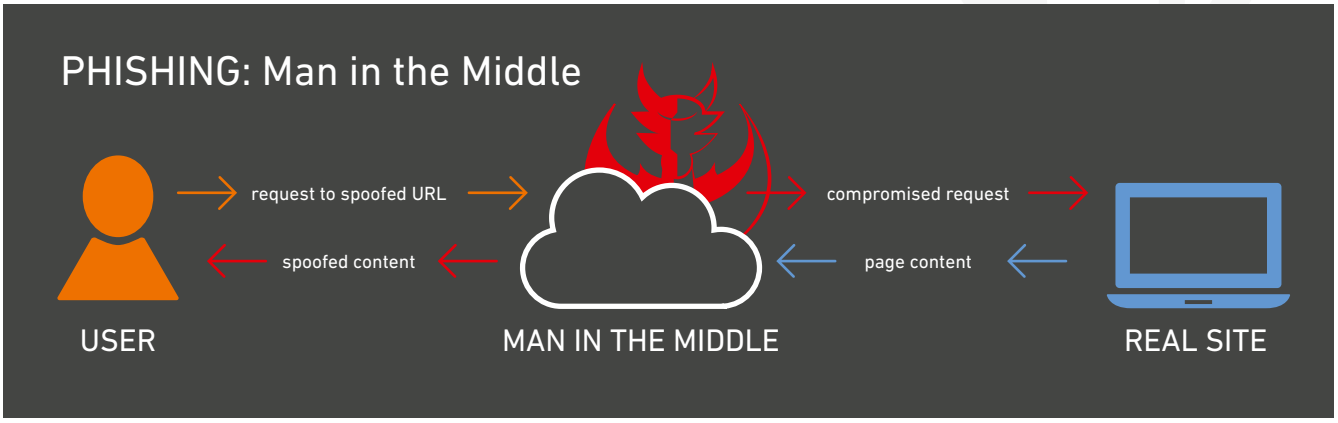

Abb. 4: Besuch einer Website bei kompromittierter Verbindung

Warum SCRYPTOS?

Da SCRYPTOS ein deutsches System ist, alle Daten ausschließlich in Rechenzentren in Deutschland gespeichert werden und keine SSL-Zertifikate von US-Unternehmen genutzt werden, besteht keine Gefahr, dass amerikanische Sicherheitsbehörden, Geheimdienste oder Unternehmen unbemerkt Zugriff auf die Daten erhalten.

Lesen Sie hierzu auch das Whitepaper „Wirtschaftsspionage als Gefahr für Hidden Champions – Nicht nur Konzerne stehen im Fokus".

Die Sicherheit Ihrer Daten steht für SCRYPTOS an höchster Stelle. Daher können Sie sich sicher sein, dass wir auch in Zukunft darauf achten werden, nur sichere Zertifikate und Rechenzentren für den Betrieb von SCRYPTOS einzusetzen.

Überzeugen Sie sich selbst und melden Sie sich noch heute für einen Testzugang auf www.scryptos.com an.

SCRYPTOS

Kontakt:
SYGNOMI GmbH
Am Kreuzstein 80 | 63477 Maintal
06109-24 54 0 | mail@sygnomi.de

Vertrieb:
SMC Consult GmbH
040-8888 299 69 | vertrieb@sygnomi.de

Autor:
Detlef Hastik

Whitepaper Version 1.0
Veröffentlichungsdatum: 01.08.2017

EINFACH VIERFACH SICHER.